



**UNITED STATES DEPARTMENT OF COMMERCE  
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

|                 |             |                      |                     |
|-----------------|-------------|----------------------|---------------------|
| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. |
|-----------------|-------------|----------------------|---------------------|

09/175,178 10/20/98 PATEL

S 13-1

TM01/0322

LUCENT TECHNOLOGIES INC  
600 MOUNTAIN AVENUE  
PO BOX 636  
MURRAY HILL NJ 07974-0636

EXAMINER

NEWTON, G

ART UNIT

PAPER NUMBER

2132

DATE MAILED:

03/22/01

**Please find below and/or attached an Office communication concerning this application or proceeding.**

**Commissioner of Patents and Trademarks**

# Office Action Summary

Application No.

09/175,178

Applicant(s)

PATEL ET AL.

Examiner

Gregory A Newton

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☐ Responsive to communication(s) filed on 20 October 1998.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☐ Claim(s) 1-3 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-3 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claims \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 10-20-78 is/are objected to by the Examiner.
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved.
- 12) ☐ The oath or declaration is objected to by the Examiner.

## Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

## Attachment(s)

- 15) ☒ Notice of References Cited (PTO-892)
- 16) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_
- 18) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 19) ☐ Notice of Informal Patent Application (PTO-152)
- 20) ☐ Other:

Art Unit: ~~2132~~ 2132

### DETAILED ACTION

1. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.
2. Claims 1 through 3 have been examined.

#### ***Specification***

3. The disclosure is objected to because of, but not limited to, the following informalities:
  4. Page 1, lines 17 and 18; page 2, lines 12 and 13. The inequality signs apparently impose no bounds on the probabilities with respect to  $\epsilon$ .
  5. Page 1, line 23: It is unclear why  $n$ , the number of bits, is called a domain.
  6. Page 4, line 21 and others: It is unknown what  $\epsilon$  stands for.
  7. Page 8, eq (9) and others: It is unknown what  $R$  stands for.
  8. It is unknown if  $p$  stands for a prime number in the claims.

Appropriate correction is required.

#### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: \*\*\*

9. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jueneman (ref 4). In Jueneman's teachings we see the square hash function, where a key is summed with a data string, then the sum is squared, then this result taken modulo some convenient prime number. Observe that in Jueneman's teachings the square hash is an iterative process that can be done more than once if desired. In the application disclosure the final result is taken modulo  $2^L$ . It is noted that this operation just means utilizing the last  $L$  bits of the result of the hash (ref 3). In fact, if  $L$  is the number of bits in the string or greater, then the noted modular operation is nothing but the identity operation, which has no effect at all. We have included some references where the noted mod operation is discussed, including the same page where Jueneman's methods are discussed in Schneier (pages 457 and 458). This operation does not change the result of the hash function, it merely discards part of it, or is due to a limiting number of bits available. Schneier also teaches that making the hash result too short will leave it vulnerable to a variety of attacks. And so, because someone with ordinary skill in the art of ciphers has an obvious motivation to decide on how many bits of the hash to keep, claim 1 is rejected in view of the Schneier reference of note and also in view of the Arnold reference.

10. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Takaragi et al. It is found in column 17 line 45 of U.S. 6,122,375 (Hash Value Generating Method.....) that Takaragi teaches the same basic hashing technique as in claim 2 of the application disclosure, where he performs the operation of summing a square hash result linearly with another key, and then takes the hash result modulo some convenient

Art Unit: \*\*\*

power of 2, which in effect determines how many bits of the hash result one wishes to keep. We have also seen where the squared quantity in the hash is known in the art as Jueneman's method. The other feature disclosed within claim 2, taking the hash result modulo some convenient number  $p$ , is not taught in the Takaragi reference. However, we can see from the prior art disclosed in the application (eqs 4 and 5, page 3) that this is a common technique in the hashing art, and so this operation is always a motivational option to one with ordinary skill in the art, and so would be obvious and commonplace. Claim 2 is rejected.

11. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jueneman's methods as taught in the Schneier reference, and further in view of Rohatgi et al (US 5,625,693), or in view of the admitted prior art, the MMH linear summation hash of equation (5) on page 3 of the Description of Related Art.

12. Claim 3 of the application discloses a summation of squares hashing technique as in the following equation: (the following equations will be understood to be modular arithmetic equations for hashing data.)

$$h(m) = \sum (a_i + m_i)^2. \quad (1)$$

But we have seen that the square hash has been taught by Jueneman's methods and so let us write the result of Jueneman's square hash as

$$m'_i(m) = (a_i + m_i)^2. \quad (2)$$

If we put this hash into the MMH hash of prior art (letting  $a_i = 1$ ), we see that

$$h(m) = \sum m'_i, \quad (3)$$

Art Unit: \*\*\*

which is nothing but the MMH hash of the prior art which is summing a plurality of Jueneman square hashes in a compositional manner. (This may also be found in the Rohatgi reference of note where he teaches a summation technique that is taken modulo 2 to some convenient power. )

It is well known that hashing is generally an iterative process whereby the argument is transformed by a series of operations, which can be a summing process, a composition of functions, multiplication, etc.(Schneier, chapter 18). And so here we have introduced a Jueneman square hash into the summation process of the prior art of note, which is nothing but combining two things from the prior art using a compositional technique. This is an obvious motivation to someone with knowledge of these techniques in the art and so claim 3 is rejected.

13. The applicants discuss the problem of collision of hashes, and the motivation to make a hash function that has low probability of collisions is found to be taught in the literature. We refer to the Transactions of the SA Institute of Electrical Engineers of June 1995, wherein the article Hash Functions Based on Modular Squaring is included herein as a reference. And so, the motivation and skill shown in the references of note show that the summation, squaring, and mod operations in the disclosure are already common motivations and as such are viewed as obvious to one of ordinary skill in the art of hashing techniques.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gregory Newton, whose telephone number is 703-305-1373. The examiner can normally be reached on M-F 9-6.

Art Unit: \*\*\*

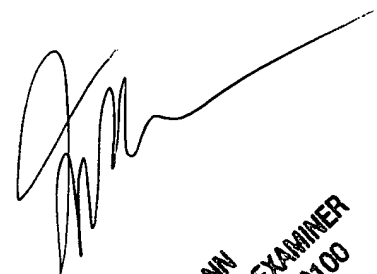
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on 703-308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are 703-308-9051 for regular communications and 703-308-9052 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.



GAN

March 19, 2001



TOD SWANN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100